Kentucky.gov

Commonwealth Office of Technology

From: Ritchey, Gail (COT)
Sent: Monday, February 04, 2008 12:13 PM
To: COT Constitutional CIO Security Contacts; COT Cabinet CIO Security Contacts; CTC Members
Cc: COT Exchange Administrators; COT Security Alert Contacts; COT Security Contact COT-Support; COT Security Contact Pass; COT Security Contact Self-Support; COT Technical Contacts; SecurityContacts Group
Subject: Targeted Spear-Phishing Attack

COT Security Alert

COT has been made aware of a spear-phishing attack which may arrive in state government user mailboxes. Spear-phishing attacks are highly targeted spam emails designed to lure users into following links or opening malicious attachments and divulging personal information for the purpose of exploitation. Using social engineering tactics and spoofed email addresses, these emails appear to come from legitimate sources with urgent messages so that users are compelled to comply with the email's request.

The current attack is associated with these attributes.

- The recipient's full name and employer may be in the message
- A malicious attachment is included that downloads keylogger software.
- A Department of Justice template is used.

The United States Department of Justice has issued a warning on it's website at http://www.usdoj.gov/atr/contact/newcase.htm concerning the current attacks.
While actions are taken to block these emails from user mailboxes, attackers commonly use methods and tools that quickly circumvent these measures.
Further recommended actions include the following:

- Educate users that such messages are fraudulent and that government entities do not communicate complaints through unsolicited emails.
- Keep software and antivirus patches and signatures up to date.
- Report suspected or confirmed infections to the Commonwealth Service Desk (502-564-7576 or CommonwealthServiceDesk@ky.gov) .

NOTICE: COT is providing this information so that you are aware of the latest security threats, vulnerabilities, software patches, etc. You should consult with your network administrator or other technical resources to ensure that the appropriate actions for these alerts are followed. If you are a network administrator and need additional information, please call the Help Desk at 502.564.7576.

Commonwealth Office of Technology
Division of Technical Services
Security Administration Branch
120 Glenn's Creek Road, Jones Building
Frankfort, KY 40601
COTSecurityServices@ky.gov
http://technology.ky.gov/security/default.htm